MATHEMATICS

UNIFORM DISTRIBUTION OF g-ADIC INTEGERS

BY

H. G. MEIJER

(Communicated by Prof. J. POPKEN at the meeting of June 24, 1967)

1. *Introduction*

This paper is the first of a series in which we develop a theory about the uniform distribution of sequences of g-adic integers. Here g stands for a fixed rational integer with $g \geqslant 2$. An exposition of the same theory, which in some places is more detailed, can already be found in the thesis of the author [8]. The present paper on the other hand contains also results not given in the thesis. Our theory includes some recent results on uniform distribution of p-adic sequences of CUGIANI [5], BERTRANDIAS [2] and CHAUVINEAU [3], [11]. Moreover, we show that the notion of uniform distribution of a sequence of rational integers, introduced by NIVEN [9], may be regarded as a special case of the notion of uniform distribution of g-adic integers. Therefore many results of NIVEN, UCHIYAMA [10] and VAN DEN EYNDEN [6] are special cases of our g-adic theorems.

The set of g-adic integers is a compact topological group with addition as the group operation. Thus uniform distribution of g-adic integers may be studied as a special case of the well-known theory of uniform distribution in a compact group. Therefore we can give many g-adic results which are only special cases of much more general theorems. We intend here, however, to give really new results and these are obtained by using the special structure of the ring of g-adic numbers.

In this paper we first review the part of the theory of g-adic numbers which is needed for our purpose (section 2). Then we define a notion of uniform distribution of sequences of g-adic integers and we illustrate it with examples of sequences which are uniformly distributed and of sequences which are not uniformly distributed (section 3). Finally, in section 4, we discuss Niven's theory on uniformly distributed sequences of rational integers.

2. *g-adic numbers*

In this section we give an introduction to the theory of g-adic numbers. For a more complete discussion we refer to MAHLER [7], chapters 1 and 2.

Definition 1. *Let R be a commutative ring. A function w, mapping R into the set of non-negative real numbers, is called a (non-archimedean) pseudo-valuation of R if it satisfies the conditions:*

a) $w(a)=0$ *if and only if* $a=0$

b) $w(ab)\leqslant w(a)w(b)$ *for all pairs* a, b; $a\in R$, $b\in R$

c) $w(a-b)\leqslant \max(w(a), w(b))$ *for all pairs* a, b; $a\in R$, $b\in R$.

If b) *may be replaced by the stronger condition*:

b′) $w(ab)=w(a)w(b)$,

then w *is called a (non-archimedean) valuation of* R.

A well-known example of a valuation is the p-adic valuation of the field Q of rational numbers. We shall denote the p-adic valuation of a rational number a by $|a|_p$. In this paper we consider, more generally, the g-adic pseudo-valuation of Q given by the next definition.

Definition 2. *Let* g *be a fixed integer*, $g\geqslant 2$, *and let*

$$g=p_1^{k_1}\,p_2^{k_2}\,\dots\,p_r^{k_r}$$

be its canonical prime factorization. For every $a\in Q$ *we define the* g*-adic pseudo-valuation* $|a|_g$ *of* a *by*

$$|a|_g=\max\{|a|_{p_1}^{\lambda_1},\dots,|a|_{p_r}^{\lambda_r}\},$$

where the real numbers $\lambda_1,\dots,\lambda_r$ *are chosen in such a way that*

$$|g|_{p_1}^{\lambda_1}=\dots=|g|_{p_r}^{\lambda_r}=g^{-1},$$

i.e. $\lambda_1=\dfrac{\log g}{k_1\log p_1},\dots,\lambda_r=\dfrac{\log g}{k_r\log p_r}$.

In the special case when g is a prime p, the g-adic pseudo-valuation evidently reduces to the p-adic valuation of Q.

Definition 3. *The ring of* g*-adic numbers* Q_g *is defined as the completion of* Q *with respect to the* g*-adic pseudo-valuation.*

Q_g has a uniquely determined pseudo-valuation which is a continuation of the g-adic pseudo-valuation on Q. (Compare [7], 9–15.) For $a\in Q_g$ we denote this pseudo-valuation by $|a|_g$. In the special case when $g=p$ is a prime the completion Q_p is the well-known field of p-adic numbers.

Definition 4. *The subset of* Q_g *consisting of all elements* a *satisfying*

$$|a|_g\leqslant 1$$

is called the ring of g*-adic integers* Z_g.

Remark 1. Every rational integer is a g-adic integer.

Theorem 1. *Every* $a\in Q_g$, $a\neq 0$, *has a unique representation*

$$a=\sum_{i=h}^{\infty}a_i g^i, \tag{1}$$

where h is a rational integer and where the a_i are taken from the set $\{0, 1, 2, \ldots, g-1\}$, $i = h, h+1, \ldots, a_h \neq 0$. *Moreover*

$$(2) \qquad |a|_g = |a_h g^h|_g = |a_h|_g g^{-h}.$$

This theorem is of fundamental importance for our investigation. In fact most of our theorems about sequences of g-adic numbers may be transferred to the case of sequences in a ring where every element can be expanded into a series of a form similar to (1). (e.g. the case of a finite algebraic extension of the field of p-adic numbers.) For a proof of the theorem we refer to [7], chapter 2.

For any integer a from the set $\{1, 2, \ldots, g-1\}$ there exists a prime divisor p_ϱ of g, such that $|a|_{p_\varrho} > |g|_{p_\varrho}$, hence such that

$$|a|_{p_\varrho}^{\lambda_\varrho} > |g|_{p_\varrho}^{\lambda_\varrho} = g^{-1}.$$

Then it follows from definition 2 and remark 1, that

$$(3) \qquad g^{-1} < |a|_g \leqslant 1 \text{ if } a \in \{1, 2, \ldots, g-1\}.$$

We can apply this inequality to the coefficients a_i in (1). In particular we note here one special case:

$$(4) \qquad \text{if } (a_i, g) = 1, \text{ then } |a_i|_g = 1.$$

We remark that the converse of the last assertion is not true.

Let a be a g-adic integer with the series representation (1). By (2) and (3) we have

$$1 \geqslant |a|_g = |a_h|_g g^{-h} > g^{-h-1}$$

and hence $h \geqslant 0$. Conversely, every g-adic number a given by (1) with $h \geqslant 0$ is a g-adic integer. Therefore the ring of g-adic integers Z_g consists exactly of those elements of Q_g such that in their series representation (1) terms with negative powers do not occur. It is often convenient to discard the condition that the first coefficient in (1) must differ from zero and to write

$$a = \sum_{i=0}^{\infty} a_i g^i \text{ for } a \in Z_g.$$

More in general we shall write

$$a = \sum_{i=-\infty}^{+\infty} a_i g^i \text{ for } a \in Q_g.$$

Then $a = 0$ has also a g-adic expansion, viz. the one in which all coefficients vanish.

Definition 5. *Let k be a fixed integer. The function ψ_k mapping Q_g into Q is defined by*

$$\psi_k(a) = \sum_{i=-\infty}^{k-1} a_i g^i,$$

where $\sum_{i=-\infty}^{+\infty} a_i g^i$ is the g-adic series of $a \in Q_g$.

Remark 2. a) For every g-adic number a, $\psi_0(a)$ is a rational number with $0 \leqslant \psi_0(a) < 1$.
b) If $a \in Z_g$ and if k is a positive integer, then

$$\psi_k(a) = \sum_{i=0}^{k-1} a_i g^i$$

is one of the integers $0, 1, 2, \ldots, g^k - 1$.

Remark 3. Let k be a positive integer and j an arbitrary (rational) integer. Then, by remark 1, j is also a g-adic integer and we have

$$\psi_k(j) \equiv j \pmod{g^k}.$$

Remark 4. If $a, b \in Z_g$ and k is a positive integer, then

$$\psi_k(a+b) \equiv \psi_k(a) + \psi_k(b) \pmod{g^k}$$
$$\psi_k(ab) \equiv \psi_k(a)\psi_k(b) \pmod{g^k}.$$

Remark 5. If $a \in Z_g$ and $(\psi_1(a), g) = 1$ then we see from remark 2b that $\psi_1(a) = a_0$, hence using (2) and (4),

$$|a|_g = 1.$$

Definition 6. *Let d be an element of Q_g, k an integer. Then we define the k-neighbourhood $U_k(d)$ of d by*

$$U_k(d) = \{x | x \in Q_g,\ |x-d|_g \leqslant g^{-k}\}.$$

We now state three lemmas which will often be used in the sequel. For the simple proofs we refer to [8], p. 14, 15.

Lemma 1. *Let k be an integer and let $a, d \in Q_g$. Then $a \in U_k(d)$ is equivalent to $\psi_k(a) = \psi_k(d)$. In other words: if d has the g-adic expansion*

$$d = \sum_{i=-\infty}^{+\infty} d_i g^i,$$

then any element $a \in U_k(d)$ has a g-adic series of the form

$$a = \sum_{i=-\infty}^{k-1} d_i g^i + \sum_{i=k}^{\infty} a_i g^i.$$

Lemma 2. *Let k be a positive integer and let $d \in Z_g$. Then there exists an integer j, $0 \leqslant j \leqslant g^k - 1$, such that $U_k(d) = U_k(j)$.*

Lemma 3. *Let k be a positive integer. Then*

$$Z_g = \bigcup_{j=0}^{g^k-1} U_k(j),$$

where the $U_k(j)$ are disjoint.

Finally, we state one more lemma about the structure of Z_g.

Lemma 4. *If a is an element of Z_g, then a is a unit of Z_g if and only if $(\psi_1(a), g)=1$. Moreover, if a is a unit of Z_g, then $|a|_g=|a^{-1}|_g=1$.*

Proof. Suppose first that a is a unit of Z_g. Then there exists an element $d \in Z_g$, such that $ad-1=0$. Then a fortiori,

$$|ad-1|_g \leqslant g^{-1},$$

hence

$$ad \in U_1(1).$$

Using lemma 1 and remark 3 and 4 we conclude

$$\psi_1(a)\, \psi_1(d) \equiv 1 \pmod g.$$

This implies

$$(\psi_1(a), g) = 1 \text{ and } (\psi_1(d), g)=1$$

and by remark 5 we get

$$|a|_g = 1, \ |d|_g = 1.$$

This proves the first part of the lemma.

Conversely, let $(\psi_1(a), g)=1$. Then it follows

$$(\psi_k(a), g) = 1 \text{ if } k \geqslant 1. \tag{5}$$

Since $\psi_k(a) \neq 0$ is a rational integer, $\psi_k^{-1}(a)$ exists in Q_g. Moreover, by (5) and definition 2 we have

$$|\psi_k^{-1}(a)|_g = 1. \tag{6}$$

If $k>t$ then we have

$$|\psi_k^{-1}(a)-\psi_t^{-1}(a)|_g = |\psi_k^{-1}(a)\, \psi_t^{-1}(a)\, (\psi_t(a)-\psi_k(a))|_g \leqslant g^{-t}.$$

Hence the sequence $(\psi_k^{-1}(a))_{k=1}^{\infty}$ is a fundamental sequence in Q_g. Since Q_g is complete $d=\lim\limits_{k\to\infty} \psi_k^{-1}(a)$ exists. Then $\psi_k(a)\,\psi_k^{-1}(a)=1$ leads in the limit to $ad=1$ and from (6) we get

$$|d|_g = \lim_{k\to\infty} |\psi_k^{-1}(a)|_g = 1 \quad \text{(see [7], p. 15)}.$$

Consider the additive group of Q_g. With the k-neighbourhoods as a countable base for the topology, Q_g is a locally compact topological group. Therefore there exists a Haar-measure μ on Q_g, which is normed by the condition

$$\mu Z_g = 1.$$

For a k-neighbourhood $U_k(d)$ in Q_g we then get

$$\mu U_k(d)=g^{-k}.$$

(For positive k this is easy to see from lemma 3.)

3. *Definition and examples*

Let $(x_n)_{n=1}^{\infty}$ be a sequence in a space M and let V be a subset of M. Further, let N denote an arbitrary positive integer. We shall denote the number of points x_n satisfying

$$x_n \in V, \ 1 \leqslant n \leqslant N,$$

by $A(V, N, (x_n))$ or, if there is no risk of confusion, simply by $A(V, N)$.

Definition 7a. *Let $(x_n)_{n=1}^{\infty}$ be a sequence in Z_g and let k be a positive integer. If*

$$\lim_{N\to\infty} N^{-1} A(U_k(d), N) = g^{-k} \tag{7}$$

for all $d \in Z_g$, then we say that the sequence is k-uniformly distributed in Z_g.

Remark 6. By lemma 2 it is sufficient that (7) holds for

$$d = 0, 1, 2, \ldots, g^k - 1.$$

Definition 7b. *A sequence $(x_n)_{n=1}^{\infty}$ in Z_g is called uniformly distributed in Z_g, if it is k-uniformly distributed in Z_g for all positive integers k.*

The next theorem will provide us with an example of a uniformly distributed sequence in Z_g.

Theorem 2. *The sequence $(1, 2, 3, \ldots)$ of positive integers is uniformly distributed in Z_g. For this sequence we even have*

$$A(U_k(d), N) = g^{-k} N + \vartheta \text{ with } |\vartheta| < 1,$$

for all $d \in Z_g$ and all positive integers k and N.

Proof. From remark 1 it follows that the sequence $(n)_{n=1}^{\infty}$ is really a sequence in Z_g.

Let k be a positive integer and let $d \in Z_g$. We have, using lemma 1 and remark 3,

$$n \in U_k(d) \text{ if and only if } n \equiv \psi_k(d) \pmod{g^k}.$$

Since $\psi_k(d)$ is an integer, we get

$$A(U_k(d), N) = [g^{-k} N] + \Delta \text{ with } \Delta = 0 \text{ or } 1 \text{ for}$$

every $d \in Z_g$. This proves the theorem.

Theorem 3. *Let $(x_n)_{n=1}^{\infty}$ be a sequence, uniformly distributed in Z_g, and let $a, b \in Z_g$. Then the sequence*

$$(a x_n + b)_{n=1}^{\infty}$$

is uniformly distributed in Z_g if and only if a is a unit of Z_g.

Proof. Let a be a unit of Z_g, then by lemma 4

$$|a|_g = |a^{-1}|_g = 1. \tag{8}$$

Now let d be an arbitrary element of Z_g. Then

$$|ax_n+b-d|_g \leqslant |a|_g\,|x_n+a^{-1}b-a^{-1}d|_g \leqslant |a|_g\,|a^{-1}|_g\,|ax_n+b-d|_g. \tag{9}$$

Combining (8) and (9) we get

$$|ax_n+b-d|_g = |x_n+a^{-1}b-a^{-1}d|_g.$$

Hence,

$$A(U_k(d),\, N,\, (ax_n+b)) = A(U_k(a^{-1}d-a^{-1}b),\, N,\, (x_n)),$$

for every positive integer k. Observe that $a^{-1}d-a^{-1}b \in Z_g$. Since $(x_n)_{n=1}^{\infty}$ s uniformly distributed in Z_g, it follows from the definitions 7a, b that $(ax_n+b)_{n=1}^{\infty}$ also is uniformly distributed in Z_g.

Suppose conversely that the sequence $(ax_n+b)_{n=1}^{\infty}$ is uniformly distributed in Z_g. Then a fortiori there exists an element x_n such that

$$ax_n+b \in U_1(1+b).$$

By lemma 1 it holds for x_n

$$\psi_1(ax_n+b) = \psi_1(1+b).$$

This implies, using remarks 4 and 3,

$$\psi_1(a)\,\psi_1(x_n) \equiv 1 \pmod{g}.$$

Therefore

$$(\psi_1(a),\, g) = 1;$$

it follows from lemma 4 that a is a unit of Z_g.

Remark 7. In the p-adic case we have $(\psi_1(a), p)=1$ if $\psi_1(a)\neq 0$. Therefore the condition $|a|_p=1$ is necessary and sufficient for a to be a unit of Z_p. Then we get the following result of Cugiani [5], p. 354, as a corollary of theorem 2 and theorem 3.

Corollary. If $a, b \in Z_p$, such that $|a|_p=1$, then the sequence $(an+b)_{n=1}^{\infty}$ is uniformly distributed in Z_p.

The next theorem gives us examples of sequences which are certainly not uniformly distributed in Z_g.

Theorem 4. *The sequence $(n^r)_{n=1}^{\infty}$, where r denotes a fixed integer, $r\geqslant 2$, is not r-uniformly distributed and hence not uniformly distributed in Z_g.*

Proof. If $|n|_g \leqslant g^{-1}$, then $|n^r|_g \leqslant g^{-r}$.

Stated otherwise: $n \in U_1(0)$ implies $n^r \in U_r(0)$; hence

$$N^{-1}A(U_r(0),\, N,\, (n^r)) \geqslant N^{-1}A(U_1(0),\, N,\, (n)).$$

By theorem 2 the right-hand side of this inequality has the limit g^{-1} as N tends to infinity. Therefore the left-hand side cannot have a limit g^{-r}.

Remark 8. By the same argument one can prove:
Let f be a polynomial of degree greater than 1 with coefficients in Z_g, such that the coefficient of the linear term vanishes. Then the sequence $(f(n))_{n=1}^{\infty}$ is not uniformly distributed in Z_g.

Now one might expect that more generally for every polynomial f over Z_g of degree greater than 1, the sequence $(f(n))_{n=1}^{\infty}$ is not uniformly distributed in Z_g. This conjecture, however, is false. As a counterexample we prove the next theorem. (Compare CHAUVINEAU [11], p. 53).

Theorem 5. *Let $a, b, c \in Z_g$ such that $|a|_g < 1$ and b is a unit of Z_g. Then the sequence*

$$(an^2+bn+c)_{n=1}^{\infty}$$

is uniformly distributed in Z_g.

Proof. If k is a positive integer and d is an arbitrary element of Z_g, then by lemma 1 and remarks 3 and 4, the relation

$$an^2+bn+c \in U_k(d)$$

is equivalent to

$$\psi_k(a)n^2+\psi_k(b)n+\psi_k(c) \equiv \psi_k(d) \pmod{g^k}. \tag{10}$$

Obviously, the sequence (an^2+bn+c) is uniformly distributed in Z_g if and only if for every positive integer k and every $d \in Z_g$ the solution of (10) is just one class of residues mod g^k.

Let f_k be the mapping of the set of integers $\{0, 1, 2, \ldots, g^k-1\}$ into itself defined by

$$f_k(n) \equiv \psi_k(a)n^2+\psi_k(b)n+\psi_k(c) \pmod{g^k}.$$

Then (an^2+bn+c) is uniformly distributed in Z_g if and only if f_k is an injection for every k. In order to prove this suppose

$$f_k(n) = f_k(m),$$

then it follows

$$(n-m)\,(\psi_k(a)\,(n+m)+\psi_k(b)) \equiv 0 \pmod{g^k}. \tag{11}$$

Let $p_1, p_2, \ldots, p_r$ be the different primes in the prime factorization of g. Since $|a|_g < 1$ we have for the rational integer $\psi_k(a)$, $|\psi_k(a)|_g < 1$, and then by definition 2

$$\psi_k(a) = 0 \text{ or } p_\varrho/\psi_k(a) \text{ for } \varrho = 1, 2, \ldots, r.$$

Further b is a unit of Z_g and then by lemma 4

$$(\psi_k(b), g) = 1.$$

Hence

$$(\psi_k(a)\,(n+m)+\psi_k(b),\, g) = 1 \text{ for all integers } n, m.$$

Then it follows from (11)

$$n \equiv m \pmod{g^k}$$

i.e. f is an injection indeed. This proves the theorem.

Remark 9. In the same way it follows: Let h be a polynomial over Z_g, b a unit of Z_g and $a \in Z_g$, such that $|a|_g < 1$. Then the sequence

$$(bn + ah(n))_{n=1}^{\infty}$$

is uniformly distributed in Z_g.

If g is an odd number, then one can prove that the converse of theorem 5 holds: Let $a, b, c \in Z_g$ such that $(an^2 + bn + c)_{n=1}^{\infty}$ is uniformly distributed in Z_g, then $|a|_g < 1$ and b is a unit of Z_g.

The next theorem puts us in a position to give many uniformly distributed sequences in Z_g.

Theorem 6. *Let $(x_n)_{n=1}^{\infty}$ be a sequence of real numbers and let k be a fixed positive integer. If the real sequence $(g^{-k}x_n)_{n=1}^{\infty}$ is uniformly distributed modulo* 1, *then the sequence $([x_n])_{n=1}^{\infty}$ considered as a sequence in Z_g, is k-uniformly distributed in Z_g.*

Proof. Let

$$[x_n] \in U_k(d) \tag{12}$$

for some $d \in Z_g$. Then by lemma 1 and remark 3

$$[x_n] \equiv \psi_k(d) \pmod{g^k}$$

or

$$g^{-k}x_n \in [g^{-k}\psi_k(d),\, g^{-k}(\psi_k(d)+1)) \pmod{1}. \tag{13}$$

Conversely, (13) implies (12). Therefore

$$A(U_k(d), N, [x_n]) = A([g^{-k}\psi_k(d),\, g^{-k}(\psi_k(d)+1)),\, N,\, (\{g^{-k}x_n\})).$$

Since by hypothesis the sequence $(g^{-k}x_n)_{n=1}^{\infty}$ is uniformly distributed modulo 1, we have

$$\lim_{N\to\infty} N^{-1}A(U_k(d), N, ([x_n]) = g^{-k},$$

which proves the theorem.

It is well-known that the following real sequences are uniformly distributed mod 1 (cf. e.g. Cigler–Helmberg [4], p. 8, 9).

1) $(\alpha n+\beta)_{n=1}^{\infty}$ where α is an irrational and β an arbitrary real number. More in general:

2) $(f(n))_{n=1}^{\infty}$ where f is a polynomial with real coefficients of which at least one, different from $f(0)$, is irrational.

3) $(\alpha n^{\sigma})_{n=1}^{\infty}$ with α, σ real, $\alpha \neq 0$, $\sigma > 0$, σ non-integral.

4) $(\alpha(\log n)^{\tau})_{n=1}^{\infty}$ with α, τ real, $\alpha \neq 0$, $\tau > 1$.

Then theorem 6 implies:

Corollaries. The following sequences are uniformly distributed in Z_g.

1) $([\alpha n+\beta])_{n=1}^{\infty}$ with α irrational real, β real.

2) $([f(n)])_{n=1}^{\infty}$ where f is a polynomial as considered above.

3) $([\alpha n^{\sigma}])_{n=1}^{\infty}$ with α, σ real, $\alpha \neq 0$, $\sigma > 0$, σ non-integral.

4) $([\alpha(\log n)^{\tau}])_{n=1}^{\infty}$ with α, τ real, $\alpha \neq 0$, $\tau > 1$.

4. *Uniform distribution of integers*

Let m be a fixed rational integer, $m \geqslant 2$ and let $(x_n)_{n=1}^{\infty}$ be a sequence of rational integers. For any integer j we denote by $A(j, N)$ the number of x_n with

$$x_n \equiv j \pmod{m}, \quad 1 \leqslant n \leqslant N.$$

Definition 8. *The sequence of rational integers $(x_n)_{n=1}^{\infty}$ is called uniformly distributed modulo m for an integer $m \geqslant 2$, if*

$$\lim_{N\to\infty} N^{-1}A(j, N) = m^{-1} \text{ for } j=0, 1, 2, \ldots, m-1.$$

If the sequence is uniformly distributed modulo m for every integer $m \geqslant 2$, then we say that $(x_n)_{n=1}^{\infty}$ is a uniformly distributed sequence of integers.

Examples.

1. The sequence $(1, 2, 3, \ldots)$ of positive integers is a uniformly distributed sequence of integers.
2. Let m, a and b be integers, $m \geqslant 2$, $(a, m)=1$. Since for any integer j the solution of the congruence $an+b \equiv j \pmod{m}$ is a class of residues modulo m, it follows that the sequence $(an+b)_{n=1}^{\infty}$ is uniformly distributed modulo m.

A theory of uniform distribution in this sense has been developed by Niven [9], [1] p. 158–160, Uchiyama [10], Van den Eynden [6] and others. Our next theorem shows that the notion of uniform distribution of sequences of integers may be regarded as a special case of the notions of uniform distribution of g-adic numbers.

Theorem 7. *Let* $(x_n)_{n=1}^{\infty}$ *be a sequence of rational integers and* m *an integer,* $m \geqslant 2$. *Then*

I. *The sequence* $(x_n)_{n=1}^{\infty}$ *is uniformly distributed mod* m *if and only if the sequence* $(x_n)_{n=1}^{\infty}$, *considered as a sequence in* Z_m, *is* 1-*uniformly distributed in* Z_m.

II. *The sequence* $(x_n)_{n=1}^{\infty}$ *is a uniformly distributed sequence of integers if and only if for every integer* $m \geqslant 2$ *the sequence* $(x_n)_{n=1}^{\infty}$, *considered as a sequence in* Z_m, *is uniformly distributed in* Z_m.

Proof.

I. Consider the sequence $(x_n)_{n=1}^{\infty}$ as a sequence in Z_m. By lemma 1 and remark 3, the relation $x_n \in U_1(j)$ is equivalent to $x_n \equiv j \pmod{m}$. Therefore

$$A(U_1(j), N) = A(j, N)$$

and part I of the theorem follows immediately.

II. Let $(x_n)_{n=1}^{\infty}$ be uniformly distributed in Z_m, for every integer $m \geqslant 2$. Then by definition it is certainly 1-uniformly distributed in Z_m and hence, by the previous part of this theorem, uniformly distributed mod m, for every $m \geqslant 2$.

On the other hand, let $(x_n)_{n=1}^{\infty}$ be a uniformly distributed sequence of integers and let m and k be integers, $m \geqslant 2$, $k \geqslant 1$. Since, by lemma 1 and remark 3, for any j from the set $\{0, 1, 2, \ldots, m^k - 1\}$ the congruence relation

$$x_n \in U_k(j)$$

is equivalent to

$$x_n \equiv j \pmod{m^k},$$

we have

$$A(U_k(j), N) = A(j, N), \quad j = 0, 1, 2, \ldots, m^k - 1.$$

The sequence $(x_n)_{n=1}^{\infty}$ is certainly uniformly distributed modulo m^k, therefore

$$\lim_{N \to \infty} N^{-1} A(U_k(j), N) = m^{-k}, \quad j = 0, 1, 2, \ldots, m^k - 1.$$

This implies that the sequence $(x_n)_{n=1}^{\infty}$ is k-uniformly distributed in Z_m. Since k and m were arbitrarily chosen with $k \geqslant 1$, $m \geqslant 2$, the sequence $(x_n)_{n=1}^{\infty}$ is uniformly distributed in Z_m for every integer $m \geqslant 2$. This completes the proof of the theorem.

A direct consequence of theorem 6 and of theorem 7, part I, is the following theorem of Van den Eynden [6].

Theorem 8. (Van den Eynden) *Let* $(x_n)_{n=1}^{\infty}$ *be a sequence of real numbers such that the sequence* $(m^{-1}x_n)_{n=1}^{\infty}$ *is uniformly distributed mod* 1 *for all positive integers* m. *Then the sequence* $([x_n])_{n=1}^{\infty}$ *is a uniformly distributed sequence of integers.*

Corollaries. The following sequences are uniformly distributed sequences of integers (compare the corollaries after theorem 6).

1) $([f(n)])_{n=1}^{\infty}$, where f is a polynomial with real coefficients of which at least one, different from $f(0)$, is irrational.

2) $([\alpha n^{\sigma}])_{n=1}^{\infty}$, with α, σ real, $\alpha \neq 0$, $\sigma > 0$, σ non-integral.

3) $([\alpha(\log n)^{\tau}]_{n=1}^{\infty}$ with α, τ real, $\alpha \neq 0$, $\tau > 1$.

A special case of 1), namely $f(n) = \alpha n + \beta$ with α irrational, has been given by NIVEN [9].

The sequence of 2), for the special case $\sigma = 1/q$, $q = 2, 3, \ldots$, is due to UCHIYAMA [10].

Mathematisch Instituut
Universiteit van Amsterdam

REFERENCES

1. Asymptotic distribution modulo 1; Papers presented at the NUFFIC international summer session in science (Nijenrode-lectures), P. Noordhoff, Groningen.
2. BERTRANDIAS, F., Ensembles remarquables d'adèles algébriques, Thèse, Paris 1965.
3. CHAUVINEAU, J., Complément au théorème métrique de Koksma dans R et dans Q_p, C. R. Acad. Sci. Paris, **260**, 6252–6255 (1965).
4. CIGLER, J., and G. HELMBERG, Neuere Entwicklungen der Theorie der Gleichverteilung, Jber. Deutsch. Math. Verein., **64**, 1–50 (1962).
5. CUGIANI, M., Successioni uniformemente distribuite nei domini p-adici, Ist. Lombardo Accad. Sci. Lett. Rend. **A 96**, 351–372 (1962).
6. EYNDEN, C. L. v. D.,The uniform distribution of sequences, Dissertation, Univ. of Oregon 1962.
7. MAHLER, K., Lectures on diophantine approximations, Part 1, University of Notre Dame 1961.
8. MEIJER, H. G., Uniform distribution of g-adic numbers, Proefschrift, Universiteit van Amsterdam 1967.
9. NIVEN, I., Uniform distribution of integers, Trans. Amer. Math. Soc. **98**, 52–61 (1961).
10. UCHIYAMA, S., On the uniform distribution of sequences of integers, Proc. Japan Acad. **37**, 605–609 (1961).
11. CHAUVINEAU, J., Sur la répartition dans R et dans Q_p, Thèse, Paris, Juin 1967.